
INTRODUCING:
KASPERSKY SECURITY FOR VIRTUALIZATION
FOR VMWARE, MICROSOFT AND CITRIX
VIRTUAL ENVIRONMENTS

SECURITY IN VIRTUAL ENVIRONMENTS: TRUE OR FALSE?

FALSE

VIRTUAL ENVIRONMENTS ARE MORE SECURE THAN PHYSICAL ENVIRONMENTS

A MALWARE ATTACK DOESN'T DISTINGUISH BETWEEN PHYSICAL AND VIRTUAL PC'S.

FALSE

CYBERCRIMINALS DON'T SPECIFICALLY TARGET VIRTUAL MACHINES

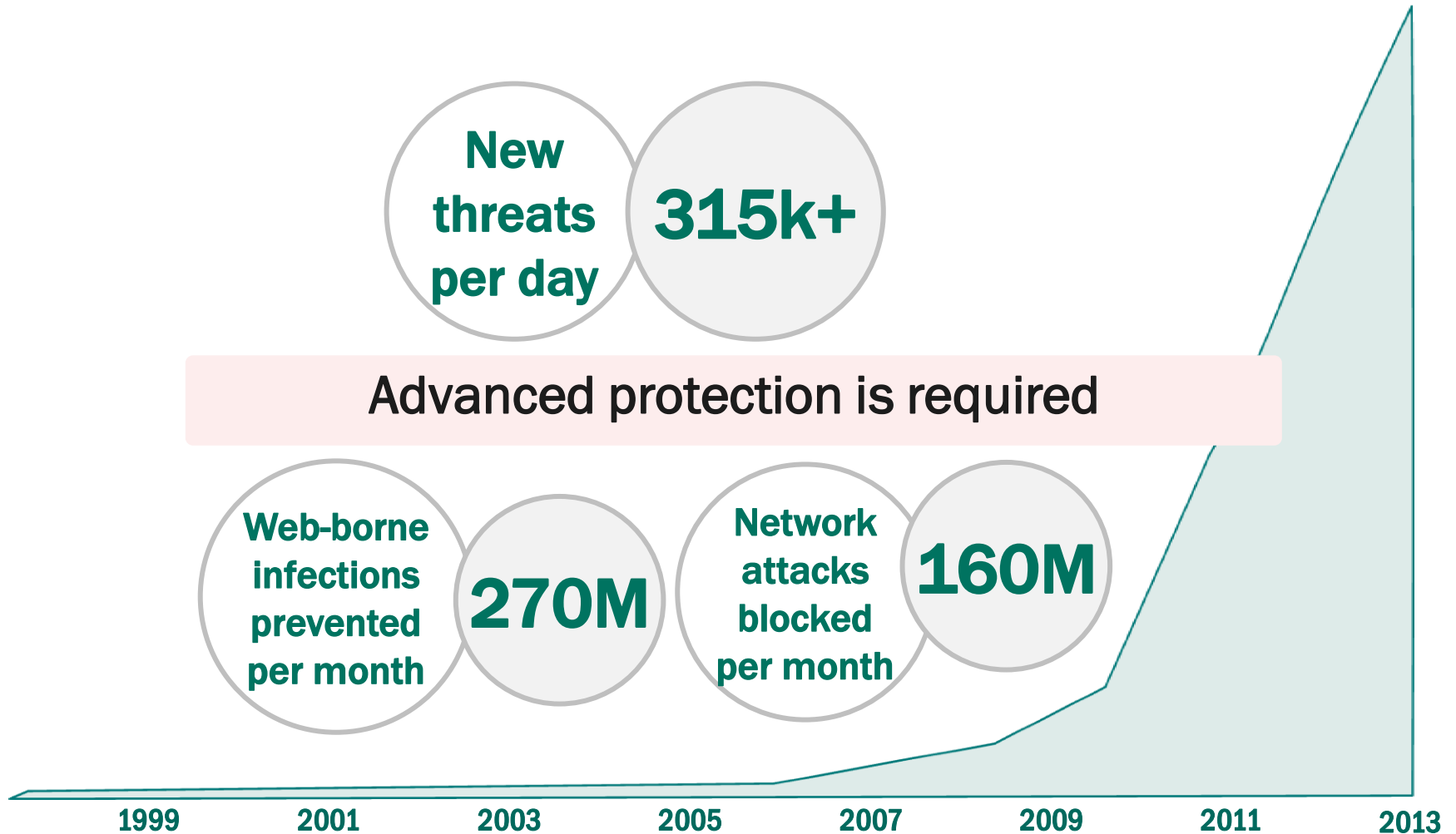
MORCUT (AKA CRISIS), THE FIRST TROJAN SPECIFICALLY TARGETING AND MOUNTING ITSELF TO VIRTUAL MACHINES ,WAS IDENTIFIED IN 2012

FALSE

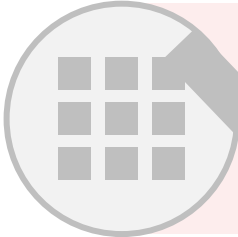
MALWARE CAN'T SURVIVE THE DECOMMISSIONING OF NON-PERSISTENT VIRTUAL MACHINES

RESIDENT MALWARE CAN. SOME MALWARE (KIDO, CONFICKER) CAN JUMP FROM VM TO VM, AND FROM HOST TO HOST.

THE GROWING MALWARE THREAT ...



VIRTUAL SECURITY – UNDERSTANDING THE OPTIONS



NO SECURITY

~~NOT AN OPTION!~~



TRADITIONAL
(Agent-Based)

GREAT PROTECTION
/INEFFICIENT
IMPLEMENTATION



AGENTLESS

EASY TO
DEPLOY/MANAGE
FOR VMWARE

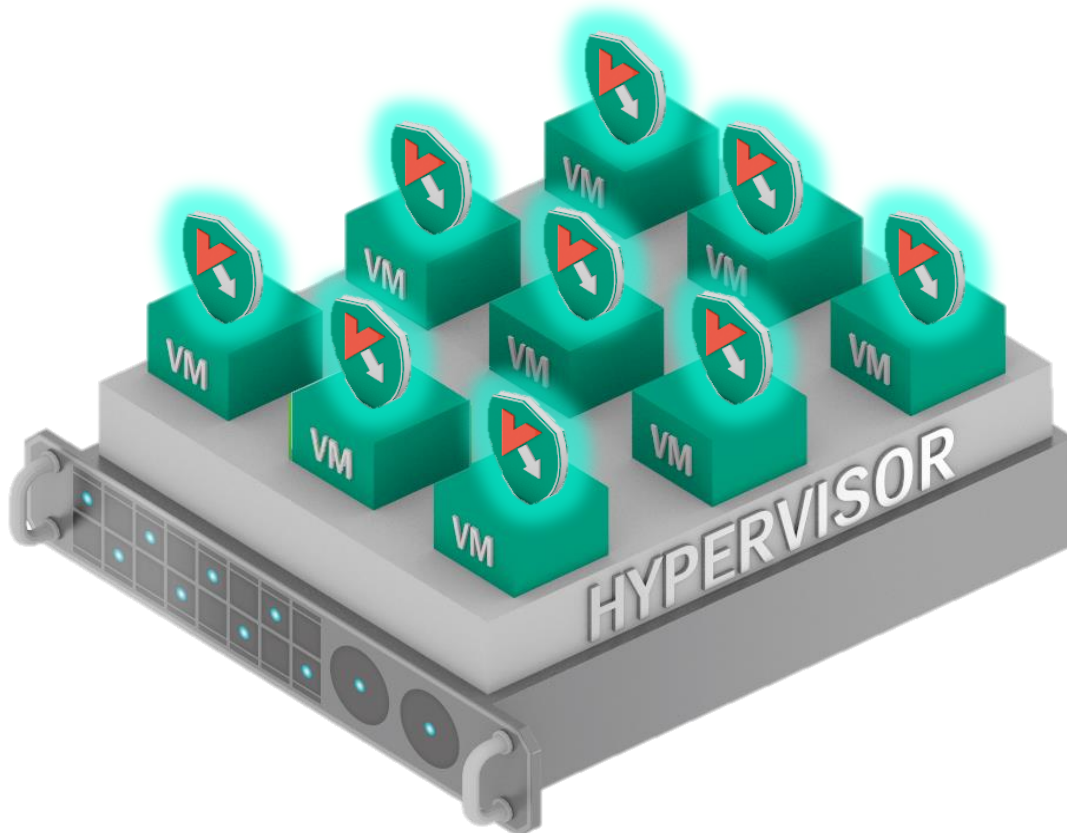


LIGHT AGENT

FEATURE-RICH
SECURITY

TRADITIONAL, AGENT-BASED SECURITY

A full version of security software is loaded on each virtual machine



Denotes an instance of security software

> Inefficient Resource Use:

- > Redundant full agents
- > Redundant Signature Databases

> Results in:

- > Excessive resource consumption
- > Update storms
- > Instant-on gaps
- > Lower VM densities

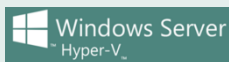
THE ANSWER - KASPERSKY SECURITY FOR VIRTUALIZATION



DESIGNED SPECIFICALLY FOR VIRTUAL ENVIRONMENTS



SINGLE PANE MANAGEMENT OF PHYSICAL, MOBILE & VIRTUAL SECURITY



SUPPORT FOR ALL KEY VMWARE, MICROSOFT AND CITRIX VIRTUALIZATION TECHNOLOGIES



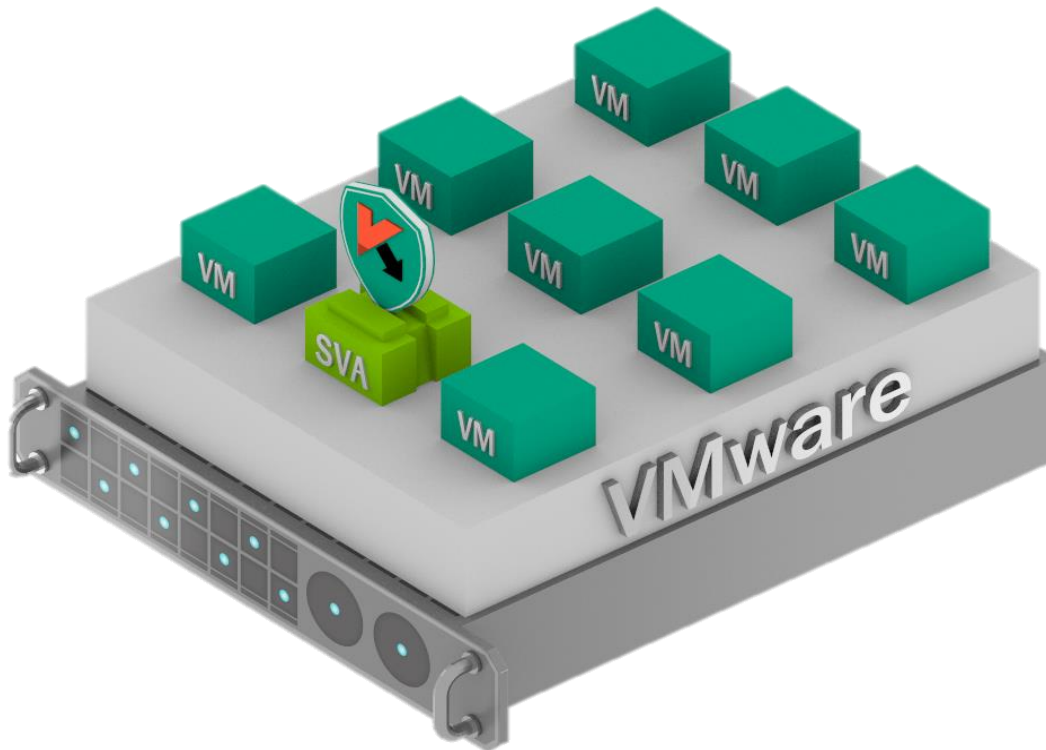
AWARD-WINNING ANTI-MALWARE ENGINE



ASSISTED BY THE KASPERSKY SECURITY NETWORK

AGENTLESS SECURITY

One Security Virtual Appliance per host performs malware scanning



> Efficient:

- > Installed and operational in under an hour
- > No re-boot or maintenance mode required

> Eliminates:

- > Excessive resource consumption
- > Update and scan storms
- > Instant-on gaps

> Results in:

- > Higher VM Densities

THE AGENTLESS APPROACH



TIGHTLY INTEGRATED WITH VMWARE



SECURITY VIRTUAL APPLIANCE SCANS FILES AND BLOCKS NETWORK ATTACKS



NO DUPLICATION OR REDUNDANCY, PRESERVING CONSOLIDATION RATIOS



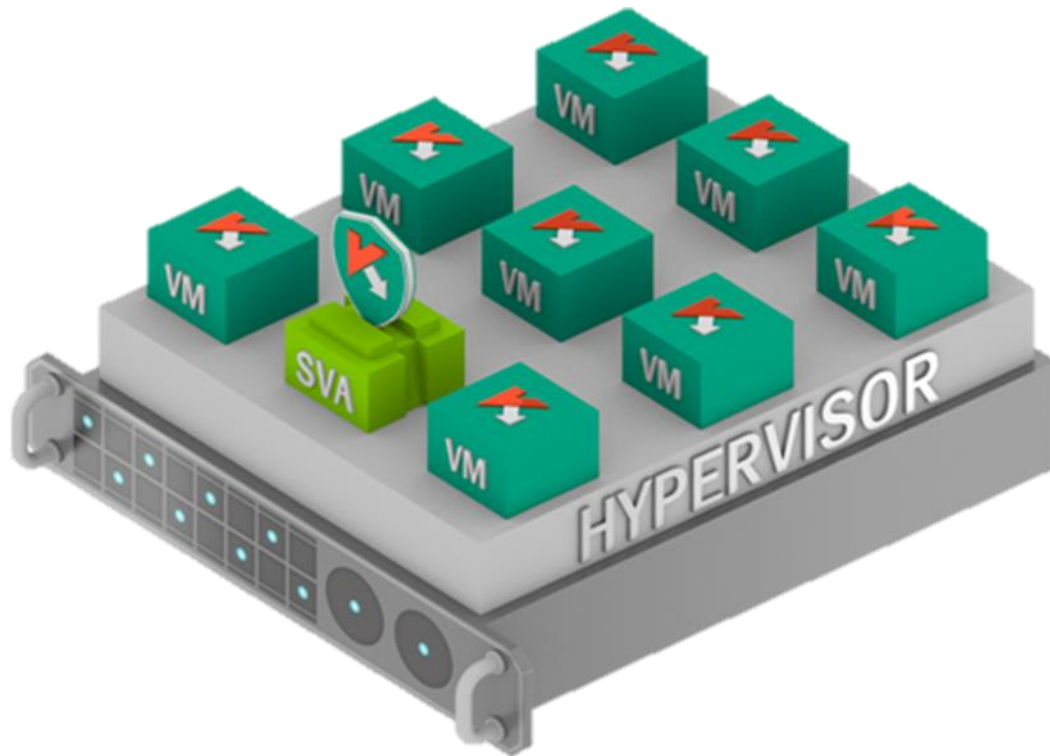
EASY TO ADMINISTER AND DEPLOY FOR INSTANT PROTECTION



EFFECTIVE IN VMWARE DEPLOYMENTS THAT REQUIRE ESSENTIAL ANTI-MALWARE PROTECTION ONLY

LIGHT AGENT SECURITY

A Security Virtual Appliance plus a lightweight security agent on each VM



- > Includes advanced security features:
 - > Vulnerability monitoring
 - > Application control
 - > Web control
 - > Device control
 - > Advanced heuristics
 - > Protection for IM, mail and web traffic
- > Eliminates:
 - > Excessive resource consumption
 - > Update and scan storms
 - > Instant-on gaps

THE LIGHT AGENT APPROACH



SUPPORT FOR VMWARE, CITRIX AND MICROSOFT HYPER-V ENVIRONMENTS



SECURITY VIRTUAL APPLIANCE SCANS FILES FOR EACH VM ON THE HOST



LIGHTWEIGHT AGENT ADDS ADVANCED SECURITY FEATURES WHILE PRESERVING CONSOLIDATION RATIOS



WEB, DEVICE AND APPLICATION POLICY ENFORCEMENT



AUTOMATIC EXPLOIT PREVENTION PREVENTS MALICIOUS CODE FROM CAPITALIZING ON VULNERABILITIES

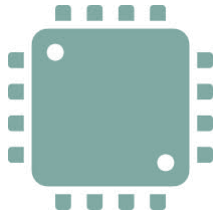
FLEXIBLE LICENSING

CHOOSE BETWEEN “PER-MACHINE” OR “PER-CORE”



PER MACHINE

License pricing based on the number of virtual machines under protection



PER CORE

License price is based upon the physical resources under protection



MULTI-PLATFORM

A license covers Hyper-V, Xen and VMware platforms

ALIGNING THE SECURITY APPROACH TO THE ENVIRONMENT

Traditional Agent-Based

- > Works on any hypervisor
- > Where VM density is not critical
- > Windows, Linux or Mac guest VMs

Agentless Security

- > VMware only
- > Allows high VM density
- > Windows guest VMs only
- > Minimal IT resources for installation and management
- > Typical installation would be server virtualization with controlled internet connectivity (no browsing)

Light Agent Security

- > VMware, Citrix or Hyper-V
- > Allows high VM density
- > Windows guest VMs
- > Advanced security requirements:
 - > IM, Web and Mail AV
 - > Automatic Exploit Prevention
 - > Application, Web and Device controls
- > Typical usage would be VDI and servers with critical roles

KASPERSKY SECURITY FOR VIRTUALIZATION OFFERS OUTSTANDING:



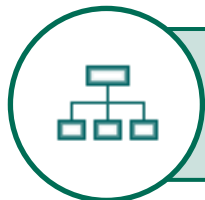
SECURITY



PERFORMANCE



EFFICIENCY



MANAGEMENT



FLEXIBILITY

THANK YOU!

Contact Kaspersky or your preferred reseller for more information on Kaspersky's virtualization security options